UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/726,952	12/03/2003	Roy Schoenberg	66729/P033US/10614705	4379

29053 7590 07/24/2009
FULBRIGHT & JAWORSKI L.L.P
2200 ROSS AVENUE
SUITE 2800
DALLAS, TX 75201-2784

EXAMINER	
SHIFERAW, ELENI A	

ART UNIT	PAPER NUMBER
2436	

MAIL DATE	DELIVERY MODE
07/24/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/726,952	SCHOENBERG, ROY	
	Examiner	Art Unit	
	ELENI A. SHIFERAW	2436	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *11 May 2009*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-22,24-28 and 30-44* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-22,24-28 and 30-44* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-22, 24-28, and 30-44 are pending, claims 37-44 are newly added and all independent claims are amended.

Response to Amendment

2. Applicant amends at least all independent claims but the non-final rejection is generated herein to address Bilski on the method claims and double patenting rejection.

Claim Rejections - 35 USC § 112

3. The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

4. Claims 1-22, 24-28, 30-44 and 37-44 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention. The amendment wherein "wherein input of the second-level access key by said medical service provider is not required" is not found in the disclosure. Appropriate correction is required.

Claim Rejections - 35 USC § 101

5. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

6. Claims (1-21 and 37-41) are rejected under 35 U.S.C. 101 based on Supreme Court precedent and recent Federal Circuit decisions, a 35 U.S.C § 101 process must (1) be tied to a particular machine or (2) transform underlying subject matter (such as an article or materials) to a different state or thing. In re Bilski et al, 88 USPQ 2d 1385 CAFC (2008); Diamond v. Diehr, 450 U.S. 175, 184 (1981); Parker v. Flook, 437 U.S. 584, 588 n.9 (1978); Gottschalk v. Benson, 409 U.S. 63, 70 (1972); Cochrane v. Deener, 94 U.S. 780,787-88 (1876).

An example of a method claim that would not qualify as a statutory process would be a claim that recited purely mental steps. Thus, to qualify as a § 101 statutory process, the claim should positively recite the particular machine to which it is tied, for example by identifying the apparatus that accomplishes the method steps, or positively recite the subject matter that is being transformed, for example by identifying the material that is being changed to a different state.

Here, applicant's method steps are not tied to a particular machine and do not perform a transformation. Thus, the claims are non-statutory.

The mere recitation of the machine in the preamble with an absence of a machine in the body of the claim fails to make the claim statutory under 35 USC 101. *Note the Board of Patent Appeals Informative Opinion Ex parte Langemyer et al.*

Applicant's claim language wherein said "datastore" is interpreted as a software according to applicant's disclosure the data store is a repository (see last 3 lines of par. 0009). Par. 0053 of the disclosure further describes that the repository(s) (**software/file/database**)

stored on a computer. Therefore applicant's datastore is interpreted as a database as collection of file/software stored on a computer and not being a hardware element/storage of the computer.

"key organization system", as recited in claim 16, is also software that is stored on a storage device 30 that is executable, according to applicant's disclosure par. 25. Therefore the claims fail to be tied to a particular machine or transform underlying subject matter (such as an **article or materials**) to a different state or thing.

Double Patenting

7. The nonstatutory double patenting rejection is based on a judicially created doctrine grounded in public policy (a policy reflected in the statute) so as to prevent the unjustified or improper timewise extension of the "right to exclude" granted by a patent and to prevent possible harassment by multiple assignees. A nonstatutory obviousness-type double patenting rejection is appropriate where the conflicting claims are not identical, but at least one examined application claim is not patentably distinct from the reference claim(s) because the examined application claim is either anticipated by, or would have been obvious over, the reference claim(s). See, e.g., *In re Berg*, 140 F.3d 1428, 46 USPQ2d 1226 (Fed. Cir. 1998); *In re Goodman*, 11 F.3d 1046, 29 USPQ2d 2010 (Fed. Cir. 1993); *In re Longi*, 759 F.2d 887, 225 USPQ 645 (Fed. Cir. 1985); *In re Van Ornum*, 686 F.2d 937, 214 USPQ 761 (CCPA 1982); *In re Vogel*, 422 F.2d 438, 164 USPQ 619 (CCPA 1970); and *In re Thorington*, 418 F.2d 528, 163 USPQ 644 (CCPA 1969).

A timely filed terminal disclaimer in compliance with 37 CFR 1.321(c) or 1.321(d) may be used to overcome an actual or provisional rejection based on a nonstatutory double patenting ground provided the conflicting application or patent either is shown to be commonly owned with this application, or claims an invention made as a result of activities undertaken within the scope of a joint research agreement.

Effective January 1, 1994, a registered attorney or agent of record may sign a terminal disclaimer. A terminal disclaimer signed by the assignee must fully comply with 37 CFR 3.73(b).

8. Claims 1-22, 24-28, and 30-44 are provisionally rejected on the ground of nonstatutory obviousness-type double patenting as being unpatentable over claim 1-36 of copending Application No.10726423. Although the conflicting claims are not identical, they are not patentably distinct from each other because the instant case, all elements of claims 11-22, 24-28, and 30-44 correspond to the claims of the copending claims and encompass the scope of claims 1-5 and 7-36 of the instant application. The instant application generally claims (**see claim 1 of 10726952**) a key maintenance method. Copending application 10726423 claims recites a key organization method and further similarly limits. For example: claim 1 of the instant application is equivalent with claims 1, 2 and 5of the copending application.

Instant application claim 1: A key maintenance method is equivalent with "receiving a second access key to the medical service provider, a patient-defining level of access,... and storing the first and second access keys, and associating the keys with the medical provider" of the copending claim 1.

"maintaining, in a datastore a first-level access key that grants, to a medical service provider, a level of access to a set of medical records of a patient;" is equivalent with "storing the first and second access keys in a centralized key repository…the first access key that grants, to the medical service provider, a patient-defined level of access to a first set of medical record" of the copending claim 1.

"retrieving the first-level access key" is equivalent with "storing the first and second access keys ….and associating … the first and second access keys" of the copending claim 1. In order to associate the first access key must be retrieved.

"generating a second-level access key by the patient modifying the level of access of the first-level access key" is equivalent with "wherein the first access key is generated by a first patient, and the first set of medical record concern the first patient" and "... allowing said medical service provider to select, from said list of patients, a corresponding patient to whom the second set of medical records pertains" of copending claims 2 and 5.

As per claim 2, each element of claim 2 of the instant application correspond to elements of claims 2 and 10 of the copending application 10726423.

As per claim 3, each element of claim 3 of the instant application correspond to elements of claim 1 of the copending application 10726423.

As per claim 4, each element of claim 4 of the instant application correspond to elements of claim 1 or 7 of the copending application 10726423.

As per claim 5, each element of claim 5 of the instant application correspond to elements of claim 1 or 7 of the copending application 10726423.

As per claim 6, each element of claim 6 of the instant application correspond to elements of claims 1 and/or 2 of the copending application 10726423.

As per claim 7, each element of claim 7 of the instant application correspond to elements of claim1 of the copending application 10726423.

And further claims 8-22, 24-28 and 30-44 are equivalent and/or encompass the scope of claims 1-5 and 7-36 of the instant application

This is a provisional obviousness-type double patenting rejection because the conflicting claims have not in fact been patented.

Claims 1-22, 24-28, and 30-44 *of the instant application would have been obvious, to one ordinary skill in the art at the time of the invention was made, over claims* 1-5 and 7-36 *of the copending application 10726423 because using equivalent wording in a different application does not make the application/invention distinct and each limitation of the claims of the instant application are anticipated/equivalent by the claims 1-5 and 7-36 of the copending application and encompass the scope of claims* 1-22, 24-28, and 30-44 *of the instant application.*

Claim Rejections - 35 USC § 103

9. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

10. Claims 1, 2, 4-6, 8-10, 13, 14, 16, 17, 19-22, 24, 26, 27, 28, 38, 40, and 44 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kohane et al. Pub. No. 2004/0199765 A1 in view of Knapton, III USPN 6363486 B1.

Regarding claim 1, Kohane et al. teaches a key maintenance **(see par. 46-61, figs. 1, and 2A-B)** method comprising:

maintaining, in a datastore **(see fig. 2B)** a first-level **(see par. 53-55)** access key **(see par. 5-8; each token is different and based on access rights that the patient provided)** that grants **(fig. 5 and par. 61)**, to a medical service provider **(par. 24 &7; the agent is a health care institution, health research facility …)**, a level of access to a set of medical records of a patient **(par. 37 and 38-43)**;

retrieving the first-level access key **(par. 79 and fig. 5; retrieving and comparing agent provided token with specified access rights)**; and

a second-level access key **(see fig. 2B; pwd_1, pwd_2 …)** by the patient modifying the level of access of the first-level access key **(see par. 46-61, and 13; the patient is controlling his own medical record (portion or all) by modifying and providing different roles/rights to different agents/doctors/health institutes)**.

Kohane et al. discloses the document owner i.e. the patient/creator/individual **(par. 37, 40, and 5-8)** selecting confidential/medical records of his own and controlling the selected portions of his own medical record **(par. 49-55)** by providing different tokens to different health institutions and doctors **(par. 7, and 49-53)** by specifying access rights/roles **(see par. 55-61 and fig. 3-6B)**. However Kohane et al. fails to explicitly disclose generating the second-level key by modifying the first level key.

Knapton, III discloses that generation of a password from first and second key **(see col. 2 lines 24-43)** and further discloses that password is generated from different information **(see col. 2 lines 24-43).**

Therefore it would have been obvious to one having ordinary skill in the art at the time of the invention was made to modify the teachings of Knapton, III within the system of Kohane et al. because they are analogous in access control. One would have been motivated to modify the teachings to generate the second key based on first access information.

Regarding claim 16, Kohane et al. teaches a key maintenance method **(see par. 46-61, figs. 1, and 2A-B)** comprising:

maintaining, in a datastore **(see fig. 2B)**, a first-level **(see par. 53-55)** access key **(see par. 5-8; plurality of passwords/tokens are provided based on plurality of different roles/rights that the patient provides to health care institutes/doctors by the patient selecting portion of his medical record see further par. 13 and 53)** that grants **(fig. 5 and par. 61)**, to a first medical service provider **(par. 24 &7; the agent is a health care institution, health research facility …)**, a first level of access to a set of medical records of a patient **(par. 37 and 38-43)**;

associating, by a key organization system that is communicatively coupled to said datastore **(see fig. 1)**, said first-level access key with said first medical service provider **(see par. 8-9, 14 and fig. 2B)**;

retrieving, by the key organization system, the first-level access key **(par. 79 and fig. 5; retrieving and comparing agent provided token with specified access rights)**;

by the key organization system, a second-level access key **(see fig. 2B; pwd_1, pwd_2 …)** by modifying the level of access of the first-level access key **(see par. 46-61)**, said second-

level access key ranting, to a second medical service provider, a second level of access to the set of medical records of the patient **(see fig. 2B, par. 7-14 and 46-55)**; and

deleting, by the key organization system, the first-level access key from the datastore **(see par. 63; the agent system deleting *all* information including *all* downloaded files, cached files ... when the agent/doctor finishes reviewing)**;

associating, by the key organization system, said second-level access key with said second medical service provider **(see fig. 2B; agent-2 is associated with pwd-2…agent-3 is associated with ped-4)**;

identifying, by said key organization system, the second medical service provider **(figs. 2B, and 4-6B)**; and

responsive to said second medical service provider requesting access to the set of medical records of the patient **(par. 76, 79, 24 and figs. 2-6B; plurality of agents/healthcare institutions/doctors stored in the list and password/token is required to access patient's medical records that the patient control access, and for each agents password/token is compared with the plurality of password stored in fig. 2B)**, said key organization system using said second-level access key for granting said second medical service provider said second level of access to the set of medical records of the patient **(fig. 5, par. 79-86 and 50-55)**.

Kohane et al. discloses the document owner i.e. the patient/creator/individual **(par. 37, 40, and 5-8)** selecting confidential/medical records of his own and controlling the selected portions of his own medical record **(par. 49-55)** by providing different tokens to different health institutions and doctors **(par. 7, and 49-53)** by specifying access rights/roles **(see par. 55-61 and**

fig. 3-6B). However Kohane et al. fails to explicitly disclose generating the second-level key by modifying the first level key.

Knapton, III discloses that generation of a password from first and second key **(see col. 2 lines 24-43)** and further discloses that password is generated from different information **(see col. 2 lines 24-43).**

Therefore it would have been obvious to one having ordinary skill in the art at the time of the invention was made to modify the teachings of Knapton, III within the system of Kohane et al. because they are analogous in access control. One would have been motivated to modify the teachings to generate the second key based on first access information.

Regarding claim 22, Kohane et al. teaches a key maintenance system **(see par. 46-61, figs. 1, and 2A-B)** comprising:

a server system including a computer processor and associated memory, the server system communicatively coupled to a centralized key repository and a centralized medical record repository **(fig. 1)**;

wherein the server system is configured to:

maintain, in a datastore **(see fig. 2B)**, a first-level **(see par. 53-55)** access key **(see par. 5-8; plurality of passwords/tokens are provided based on plurality of different roles/rights that the patient provides to health care institutes/doctors by the patient selecting portion of his medical record see further par. 13 and 53)** that grants **(fig. 5 and par. 61)**, to a medical service provider **(par. 24 &7; the agent is a health care institution, health research facility …)**, a level of access to a set of medical records of a patient **(par. 37 and 38-43)**;

retrieve the first-level access key **(par. 79 and fig. 5; retrieving and comparing agent provided token with specified access rights)**; and

a second-level access key **(see fig. 2B; pwd_1, pwd_2 …)** by modifying the level of access of the first-level access key **(see par. 46-61)**;

store the second-level access key in the datastore **(see fig. 2B; plurality of access keys with different roles/rights stored)**; and

wherein said server system is further configured to, responsive to receipt of a request by the medical service provider to access the set of medical records of the patient, use the second-level access key to grant said medical service provider the modified level of access **(fig. 5, par. 79-86 and 50-55)**.

Kohane et al. discloses the document owner i.e. the patient/creator/individual **(par. 37, 40, and 5-8)** selecting confidential/medical records of his own and controlling the selected portions of his own medical record **(par. 49-55)** by providing different tokens to different health institutions and doctors **(par. 7, and 49-53)** by specifying access rights/roles **(see par. 55-61 and fig. 3-6B)**. However Kohane et al. fails to explicitly disclose generating the second-level key by modifying the first level key.

Knapton, III discloses that generation of a password from first and second key **(see col. 2 lines 24-43)** and further discloses that password is generated from different information **(see col. 2 lines 24-43).**

Therefore it would have been obvious to one having ordinary skill in the art at the time of the invention was made to modify the teachings of Knapton, III within the system of Kohane et

al. because they are analogous in access control. One would have been motivated to modify the teachings to generate the second key based on first access information.

Regarding claim 2, Kohane et al. teaches the key maintenance method wherein: the levels of access of the first-level and second-level access keys are defined using one or more access parameters **(see fig. 4-6B);**

the set of medical records is a multi-portion medical record (**see par. 13, 32 and 53)**; and

the access parameters provide access to one or more portions of the set of medical records **(see par. 13-14 and 53)**.

Regarding claim 4, Kohane et al. teaches the key maintenance method further comprising storing the second-level access key in the datastore **(see fig. 2B).**

Regarding claim 5, Kohane et al. teaches the key maintenance method further comprising deleting the first-level access key from the datastore **(see par. 63; the agent system deleting *all* information including *all* downloaded files, cached files ... when the agent/doctor finishes reviewing)**.

Regarding claims 6, 17, and 24, Kohane et al. teaches the key maintenance method wherein the datastore is a patient key repository assigned to the patient **(see fig. 2B).**

Regarding claims 8, 19, and 26, Kohane et al. teaches the key maintenance method wherein:

the patient key repository is a first portion of a centralized key repository; and the MSP key repository is a second portion of the centralized key repository **(see fig. 2B; the table with owner pwd repository and staff pwd repository, and research pwd repository …)**.

Regarding claims 9, 20, and 27, Kohane et al. teaches the key maintenance method wherein the centralized key repository resides on and is executed by a remote server connected to a distributed computing network **(see fig. 1 and 2B)**.

Regarding claims 10, 21, and 28, Kohane et al. teaches the key maintenance method wherein: the remote server is a web server; and the distributed computing network is the Internet **(see fig. 1 and 2A)**.

Regarding claim 13, Kohane et al. teaches the key maintenance method wherein the second-level access key enhances the level of access of the first level access key, wherein the medical service provider is granted a greater level of access to the set of medical records of the patient **(fig. 2B, par. 53-63 and 102-105)**.

Regarding claim 14, Kohane et al. teaches the key maintenance method wherein the second-level access key reduces the level of access of the first level access key, wherein the medical service provider is granted a reduced level of access to the set of medical records of the patient **(see par. 73-76).**

Regarding claim 38 Kohane et al. teaches the method wherein further comprising:

associating, by the key organization system, said second-level access key with a corresponding medical service provider for whom the modified level of access is granted by the patient (see fig. 2A-***6B***);

identifying, by said key organization system, said corresponding medical service provider as logging in to the key organization system **(fig. 5)**; and

responsive to said corresponding medical service provider requesting access to the set of medical records of the patient, said key organization system using said second-level access key for granting said corresponding medical service provider said modified level of access to the set of medical records of the patient **(par. 79-86 and 53-55).**

Regarding claim 40 Kohane et al. teaches key maintenance method of claim 16 wherein said first medical service provider and said second medical service provider are the same medical service provider **(par. 7-13).**

Regarding claim 44 Kohane et al. teaches the method wherein said second-level access key is not stored locally to a client computer of said medical service provider **(see fig. 2B; the table is not in the patient client).**

11. Claims 30-33, 37, 39, and 41-43 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kohane et al. Pub. No. 2004/0199765 A1 and Knapton, III USPN 6363486 B1 and further in view of Peterson US PG Pubs. 2003/0074564 A1.

Regarding claim 30, Kohane et al. teaches a computer program product residing on a computer readable medium of a server that is communicatively coupled to a communication network, said computer program product having a plurality of instructions stored thereon which, when executed by a processor of said server, cause that processor to:

maintain, in a datastore **(see fig. 2B)** that is communicatively coupled to said server **(see fig. 1)**, a first-level **(see par. 53-55)** access key **(see par. 5-8; plurality of passwords/tokens are provided based on plurality of different roles/rights that the patient provides to health care institutes/doctors by the patient selecting portion of his medical record see further par. 13 and 53)** that grants **(fig. 5 and par. 61)**, to a medical service provider **(par. 24 &7; the agent is a health care institution, health research facility …)**, a level of access to a set of medical records of a patient **(par. 37 and 38-43)**;

receive, via said communication network, a request from said patient to modify the level of access granted to the medical service provider by the first- level access key **(see par. 73-81)**;

retrieve the first-level access key **(par. 79 and fig. 5; retrieving and comparing agent provided token with specified access rights)**;

a second-level access key **(see fig. 2B; pwd_1, pwd_2 …)** by modifying the level of access of the first-level access key as specified in the received request from said patient **(see par. 46-61)**;

identify the medical service provider **(see fig. 4-6B)**;

receive, via said communication network, a request from said medical service provider to access the set of medical records of the patient **(see par. 79-83)**; and

responsive to said received request, use said second-level access key for granting said medical service provider the modified level of access to the set of medical records of the patient **(fig. 5, par. 79-86 and 50-55)**.

Kohane et al. discloses the document owner i.e. the patient/creator/individual **(par. 37, 40, and 5-8)** selecting confidential/medical records of his own and controlling the selected portions of his own medical record **(par. 49-55)** by providing different tokens to different health institutions and doctors **(par. 7, and 49-53)** by specifying access rights/roles **(see par. 55-61 and fig. 3-6B)**. However Kohane et al. fails to explicitly disclose generating the second-level key by modifying the first level key.

Knapton, III discloses that generation of a password from first and second key **(see col. 2 lines 24-43)** and further discloses that password is generated from different information **(see col. 2 lines 24-43).**

Therefore it would have been obvious to one having ordinary skill in the art at the time of the invention was made to modify the teachings of Knapton, III within the system of Kohane et al. because they are analogous in access control. One would have been motivated to modify the teachings to generate the second key based on first access information.

The combination of Kohane et al. and Knapton, III fail to teach wherein input of the second-level access key by said medical service provider is not required.

However Peterson discloses no requirement of password entry by doctors at an emergency to view patient's records **(see par. 29 and abstract last 2 lines).**

Therefore it would have been obvious to one having ordinary skill in the art at the time of the invention was made to modify the teachings of Peterson within the combination system

because they are analogous in access control. One would have been motivated to include the teachings to facilitate access in the event of emergency or urgent care situation.

Regarding claim 31, Kohane et al. teaches the key maintenance method further comprising storing the second-level access key in the datastore **(see fig. 2B).**

Regarding claim 32, Kohane et al. teaches the key maintenance method further comprising deleting the first-level access key from the datastore **(see par. 63; the agent system deleting *all* information including *all* downloaded files, cached files ... when the agent/doctor finishes reviewing)**.

Regarding claim 33, Kohane et al. teaches the key maintenance method wherein the datastore is a patient key repository assigned to the patient **(see fig. 2B).**

Regarding claim 37 Peterson further teaches wherein said retrieving and generating are performed by a key organization system that is communicatively coupled to said datastore (par. 18). Therefore it would have been obvious to one having ordinary skill in the art at the time of the invention was made to combine the teachings of well known key generation at any devices (server or user/patient).

Regarding claims 39, 41 and 43 Peterson teaches the method wherein said key organization system does not require input by said corresponding medical service provider of said second-

level access key **(see par. 29 and abstract last 2 lines)**. The rational for combining are the same as claim 30 above.

Regarding claim 42 Peterson teaches the system wherein said medical service provider does not supply the second-level access key to the server system **(see par. 29 and abstract last 2 lines)**. The rational for combining are the same as claim 30 above.

12. **Claims 3, 7, 18, and 25 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kohane et al. Pub. No. 2004/0199765 A1 and Knapton, III USPN 6363486 B1 and further in view of USPN Prihoda et al. USPN 6789195 B1**

Regarding claims 3, 7, 18, and 25, Kohane et al. teaches the key maintenance method further comprising transmitting the second-level access key to the medical service provider **(par. 7). Kohane et al. fails to teach** wherein the medical service provider subsequently stores the second-level access key on a medical service provider_(MSP) key repository assigned to the medical service provider. However Prihoda et al. discloses wherein the medical service provider subsequently stores the second-level access key on a medical service provider_(MSP) key repository assigned to the medical service provider **(see col. 7 lines 23-40)**. Therefore it would have been obvious to one having ordinary skill in the art at the time of the invention was made to modify the teachings to sore the key provided to the doctor because it is well known to store own key in a device.

13. **Claims 11, 12 and 15 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kohane et al. Pub. No. 2004/0199765 A1 and Knapton, III USPN 6363486 B1 and further in view of Resnitzky 20040068650.**

Regarding claims 11 and 12 the combination fails to teach wherein further comprising reconciling (includes overwriting the first-level access key stored within the MSP key repository with the second-level access key stored in the patient key repository) the patient key repository and the MSP key repository. However Resnitzky discloses the missing limitation(s) on par. 131-132. Therefore it would have been obvious to one having ordinary skill in the art at the time of the invention was made to modify the teachings of reconciling to secure the system when key is no longer needed to be provided for access reconciling enhances security.

Regarding claim 15 Resnitzky further teaches the method wherein the second-level access key revokes the level of access of the first level access key, wherein the medical service provider is prohibited from accessing the set of medical records of the patient (see par. 131-132). The rational for combining are the same as claim 11 above.

14. Claim 34 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kohane et al. Pub. No. 2004/0199765 A1, Knapton, III USPN 6363486 B1, and Peterson US PG Pubs. 2003/0074564 A1 and further in view of USPN Prihoda et al. USPN 6789195 B1

Regarding claim 34 Kohane et al. teaches the key maintenance method further comprising transmitting the second-level access key to the medical service provider **(par. 7). Kohane et al.**

fails to teach wherein the medical service provider subsequently stores the second-level access key on a medical service provider (MSP) key repository assigned to the medical service provider. However Prihoda et al. discloses wherein the medical service provider subsequently stores the second-level access key on a medical service provider (MSP) key repository assigned to the medical service provider **(see col. 7 lines 23-40)**. Therefore it would have been obvious to one having ordinary skill in the art at the time of the invention was made to modify the teachings to sore the key provided to the doctor because it is well known to store own key in a device.

15. **Claims 35 and 36 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kohane et al. Pub. No. 2004/0199765 A1 and Knapton, III USPN 6363486 B1 and Peterson US PG Pubs. 2003/0074564 A1. and further in view of Resnitzky 20040068650.**

Regarding claims 35 and 36 the combination fails to teach wherein further comprising reconciling (includes overwriting the first-level access key stored within the MSP key repository with the second-level access key stored in the patient key repository) the patient key repository and the MSP key repository. However Resnitzky discloses the missing limitation(s) on par. 131-132. Therefore it would have been obvious to one having ordinary skill in the art at the time of the invention was made to modify the teachings of reconciling to secure the system when key is no longer needed to be provided for access reconciling enhances security.

Conclusion

16. Any inquiry concerning this communication or earlier communications from the examiner should be directed to ELENI A. SHIFERAW whose telephone number is (571)272-3867. The examiner can normally be reached on Mon-Fri 8:00am-5:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser R. Moazzami can be reached on (571) 272-4195. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Eleni A Shiferaw/
Examiner, Art Unit 2436